
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

---

**JOINT APPLIED PROJECT**

---

# AN ANALYSIS OF CYBER SECURITY AND HOW IT IS AFFECTING A CONTRACT WRITING SYSTEM, SEAPORT

---

**June 2016**

**By:** **Bill Turner**
**Daniel Belcher**
**Danielle Allen**

**Advisors:** **Raymond Jones**
**Stacy McQuage**

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | *Form Approved OMB No. 0704-0188* |
|---|---|---|---|



| **1. AGENCY USE ONLY** *(Leave blank)* | **2. REPORT DATE** June 2016 | **3. REPORT TYPE AND DATES COVERED** Joint applied project |
|---|---|---|

| | |
|---|---|
| **4. TITLE AND SUBTITLE** AN ANALYSIS OF CYBER SECURITY AND HOW IT IS AFFECTING A CONTRACT WRITING SYSTEM, SEAPORT | **5. FUNDING NUMBERS** |
| **6. AUTHOR(S)** Bill Turner, Daniel Belcher, & Danielle Allen | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Naval Postgraduate School Monterey, CA 93943-5000 | **8. PERFORMING ORGANIZATION REPORT NUMBER** |
| **9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)** N/A | **10. SPONSORING / MONITORING AGENCY REPORT NUMBER** |

**11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____NPS.2016.0049-IR-EM2-A____.

| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** Approved for public release; distribution is unlimited | **12b. DISTRIBUTION CODE** |
|---|---|

**13. ABSTRACT (maximum 200 words)**

The purpose of this paper is to research cyber security and whether it creates inefficiencies and ineffective business support for the DOD—specifically, the contract writing system SeaPort. Is cybersecurity becoming too restrictive, making the ability to support the programs and warfighters inefficient and ineffective? What business practices could be put in place to protect the DOD without hindering contract and business support to the warfighter? This research topic came about due to the underperformance of SeaPort when used by NAVSEA contract specialists at Dahlgren. The research begins with a brief overview of the Internet, cyber security, and SeaPort contract writing system. The literature review describes the private and public sectors with regard to cyber security as well as any policies related to cyber security. Sixteen (16) SeaPort users were surveyed in order to gain an understanding of the issues surrounding SeaPort. We discovered that SeaPort, indeed, was having issues regarding PDF generation, FPDS-NG reporting, and overall latency. A direct correlation between cyber security and SeaPort efficiency could not be proven; however, theoretically, cyber security can be attributed. Recommendations include adding more servers to existing SeaPort network infrastructure and further research conducted by cyber experts within the government with the authority to access direct cyber reports on the system.

| **14. SUBJECT TERMS** SeaPort, cyber security, help desk, speed, cyber threat, cyber attack | **15. NUMBER OF PAGES** 65 |
|---|---|
| | **16. PRICE CODE** |

| **17. SECURITY CLASSIFICATION OF REPORT** | **18. SECURITY CLASSIFICATION OF THIS PAGE** | **19. SECURITY CLASSIFICATION OF ABSTRACT** | **20. LIMITATION OF ABSTRACT** |
|---|---|---|---|
| Unclassified | Unclassified | Unclassified | UU |

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

# AN ANALYSIS OF CYBER SECURITY AND HOW IT IS AFFECTING A CONTRACT WRITING SYSTEM, SEAPORT

Bill Turner, Civilian, Department of the Navy
Daniel Belcher, Civilian, Department of the Navy
Danielle Allen, Civilian, Department of the Navy

Submitted in partial fulfillment of the requirements for the degree of

**MASTER OF SCIENCE IN CONTRACT MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL**
**June 2016**

Approved by: Raymond Jones

Stacy McQuage

Matthew Kremer
Academic Associate
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

# AN ANALYSIS OF CYBER SECURITY AND HOW IT IS AFFECTING A CONTRACT WRITING SYSTEM, SEAPORT

## ABSTRACT

The purpose of this paper is to research cyber security and whether it creates inefficiencies and ineffective business support for the DOD—specifically, the contract writing system SeaPort. Is cybersecurity becoming too restrictive, making the ability to support the programs and warfighters inefficient and ineffective? What business practices could be put in place to protect the DOD without hindering contract and business support to the warfighter? This research topic came about due to the underperformance of SeaPort when used by NAVSEA contract specialists at Dahlgren. The research begins with a brief overview of the Internet, cyber security, and SeaPort contract writing system. The literature review describes the private and public sectors with regard to cyber security as well as any policies related to cyber security. Sixteen (16) SeaPort users were surveyed in order to gain an understanding of the issues surrounding SeaPort. We discovered that SeaPort, indeed, was having issues regarding PDF generation, FPDS-NG reporting, and overall latency. A direct correlation between cyber security and SeaPort efficiency could not be proven; however, theoretically, cyber security can be attributed. Recommendations include adding more servers to existing SeaPort network infrastructure and further research conducted by cyber experts within the government with the authority to access direct cyber reports on the system.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| APT | Advanced Persistent Threat |
| ARPANET | Advanced Research Projects Agency Network |
| AV | Anti-Virus |
| C4ISR | Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance |
| CAC | Common Access Card |
| CEO | Chief Executive Officer |
| CNBC | Consumer News and Business Channel |
| CPM | Cross-Platform Malware |
| DDOS | Distributed Denial of Service |
| DHS | Department of Defense |
| DOD | Department of Homeland Security |
| DoDIN | Department of Defense Information Network |
| DOS | Denial of Service |
| FPDS-NG | Federal Procurement Data System-Next Generation |
| FY | Fiscal Year |
| GB | Gigabyte |
| IDIQ | Indefinite Delivery Indefinite Quantity |
| IT | Information Technology |
| JIE | Joint Information Environment |
| MAC | Multiple Award Contract |
| MFA | Multifunction Authentication |
| MIT | Massachusetts Institute of Technology |
| NASA | National Astronautics and Space Administration |
| NAVSEA | Naval Sea Systems Command |
| NBC | National Broadcasting Company |
| NMCI | Navy Marine Corp Internet |
| NSWCDD | Naval Surface Warfare Center, Dahlgren Division |

| | |
|---|---|
| OPM | Office of Personnel Management |
| OSD | Office of the Secretary of Defense |
| PDF | Portable Document Format |
| PEO | Program Executive Offices |
| PII | Personally Identifiable Information |
| PSS | Professional Support Services |
| R&D | Research and Development |
| SPS | Standard Procurement System |
| SSL | Secure Socket Layer |
| TCP/IP | Transmission Control Protocol and Internet Protocol |
| TFCA | Task Force Cyber Awakening |
| UMUC | University of Maryland University College |

# EXECUTIVE SUMMARY

A recent increase in cyber incidents has led to an increased focus of the DOD on securing network systems and preventing unauthorized accesses to electronic platforms. This research examines the extent to which cyber security has affected the day-to-day operations of SeaPort and the ability of contract's departments to continue supporting DOD program operations. The purpose of this research is to provide an analysis of how that increased focus on cyber security is having an impact on a contract writing system used by the Department of Navy and Marine Corp at eight (8) commands made up of more than one-hundred twenty (120) field activities across the world. Because the DOD's spending trends have shifted from a predominately goods, supplies and equipment acquisition to a heavier focus on services acquisition, and SeaPort is a mandated portal for Navy competitive services acquisition, this research is directly tied to day-to-day support operations of the warfighter. Between the characteristics of DOD acquisition described above and the current situation, in regards to the poor performance, of the SeaPort contract writing system, it is now more important to determine whether or not there is a correlation between the uptick in cyber security focus in the federal government and the performance of business systems used to make the support of the DOD more efficient and effective. Furthermore, could it be possible that new business practices and policies be put in place in order to better support the DOD programs that require contract support in order to develop, enhance, and maintain weapon systems for the warfighter?

After developing our topic through direct day-to-day experience with the issues faced in using Seaport, we strategized a way to best gather information pertaining to the topic. Due to the tight restrictions on actual cyber-security measures being put in place in the DOD, it was realized a complete deep dive of the cyber-security environment would lead to an inability to absolutely link cyber security to the issues that SeaPort users face daily would be. We could, however, research and find information that linked cyber-security measures to poor or degraded performance of an application such as SeaPort and draw a link between those issues.

Our literature review included reviews of federal government strategies such as the White House, DOD, and Navy, articles and published documentation from private industry cyber experts, and published information and actual experience and knowledge on the SeaPort system. The government published policies and strategies provided an idea of what the government and DOD intended to do to address the concerns of cyber threats and cyber attacks. The government strategies include increasing coordination between government agencies and private industry to share vital knowledge in identifying potential attacks, increasing education of the workforce on cyber-security measures, and developing a network of experts within the government intelligence community to combat cyber warfare. The published articles on cyber security among private industry provided insight which is expected to be gained through greater coordination of government agencies and private companies. It allowed us to not only understand and describe the importance of cyber security, but it also provided evidence of a link between cyber-security measures, system infrastructures, and overall system performance. The research further describes the pitfalls of over-burdening a system without properly developing and implementing a network or server infrastructure.

By identifying this information in our research we then developed the link between cyber security and network infrastructure with SeaPort. Is the server infrastructure for the SeaPort application adequate, or should it be up-scaled to match the number of requests that are put on the application each day? Is the system used enough to up-scale the system in order to reduce bottlenecking due to lack of bandwidth? Is the system developed in such a way that bottlenecking and reduced bandwidth is used to protect the integrity of the network and the data passed across that network?

Our data collection further supports the idea that there is some form of bottlenecking, limited bandwidth, or poorly planned system infrastructure that causes inefficiencies in awarding and funding critical support contracts for the DOD programs that directly arm and support our warfighters. Unfortunately, due to the restrictions on cyber information on specific systems and networks within the DOD we can only conclude that there is a high possibility of a link between the increased focus on cyber security and poor performance of business systems used to support the warfighter.

Therefore, with evidence of that link, it can be noted that cyber security measures may in fact be affecting the efficiency and effectiveness of the DOD's contract's writing staff and therefore inadvertently negatively impacting and endangering the programs and warfighter these cyber measures are in place to protect.

THIS PAGE INTENTIONALLY LEFT BLANK

# ACKNOWLEDGMENTS

We would like to take this opportunity to thank both Ray Jones and Stacy McQuage for being our advisors for this project. Your support, time and effort have been greatly appreciated. We would like to thank all of our professors at Naval Postgraduate School and Ms. Rhonda Spelbring for their support and guidance throughout the program. Finally, we would want to thank the Head of Contracting at the Naval Surface Warfare Center, Dahlgren Division (NSWCDD) Tom Duval, our division heads, friends, and family for allowing us the opportunity to complete this program as well as for their support.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

With the recent increase and focus on cyber-security measures, inspired by cyber attacks on places such as Home Depot, Target, and even the federal government's Office of Personnel Management (OPM) twice, once in early 2015 and the other in June of 2015 (OPM, 2015). Due to the surge in cyber attacks, the president, in his February 2013 state of the Union Address, announced there would be a new national cyber-security measure that would be implemented by executive order. The order would take affect by June 2013. The executive order makes it possible for government intelligent agencies to share information about potential cyber security concerns with private companies in charge of reviewing and protecting the nation's infrastructure. The order gives companies the choice to receive the information. The growing environment of interconnectivity used to complete tasks and the ever-present risk of the Department of Defense's (DOD's) information falling into the wrong hands, just as personal information of millions has been affected by the attacks on private industry and our public sector, leaves the DOD reeling to find a solution to protect its secrets.

To determine how cyber security truly affects the DOD and its ability to provide sufficient warfighter support across the globe, we intend to focus our research on major topic areas of cyber-security measures currently implemented in the Navy, specifically the Naval Sea Systems Command (NAVSEA), and the effect of those cyber-security measures on the business systems used to support the warfighter. In this case, supporting the warfighter is the ability to provide contracting and business support to the DOD's top research and development facilities, engineering and maintenance to fielded weapons systems and assets, and training and preparedness support to the warfighters expected to use those weapons.

With the world becoming more and more interconnected, everyday systems such as SeaPort that operate on the Internet become associated with cyber security. Anyone across the world with a piece of equipment as small as a cell phone can access the Internet at any time. With a network available to anyone, it can be expected that the network could be used for good or bad. Since SeaPort is a network-driven system,

interlinking computers across the world just as the Internet does, it brings in to question the overall security of the system. As soon as information can be passed across the world through the use of the Internet the DOD enters into an area of risk. Once these risks are identified in a system within the DOD, policy makers and information assurance managers must take action to tighten the reins on the system to ensure nothing is leaked to our enemies. The questions then become, when does implementing cyber-security measures become too restrictive, and is there an acceptable amount of risk? Unfortunately, these questions are too subjective to answer; however, we can bring to light the inefficiencies brought to the table by implementing overly restrictive cyber-security measures and recommend other business practices that could be put in place to still mitigate the risk of cyber threats and still provide effective and efficient contracting support to the warfighter.

As contract specialists in the DOD, at the NSWCDD, part of the larger NAVSEA command, we use SeaPort in our day-to-day operations. As of 2014, DOD spending in services has surpassed spending on weapons systems procurements. This means that not only the NSWCDD spends more time doing services acquisition, but most commands spend a large amount of time preparing service requirements and spending money on service acquisition. In field activities such as the NSWCDD, we have been mandated to use SeaPort for all competitive, engineering-support type services. Additionally, SeaPort is used outside of the Navy, including Marine Corp Systems Commands who capitalize on the economies of scale within the system.

With the number of commands, field activities, and private industry firms entering the SeaPort network in order to fulfill a requirement, or compete for a piece of the growing DOD service sector, the system, due to its internal controls, has come to work at a slow pace. This pace is the opposite of what is necessary in order to do more with less within the DOD. Meanwhile, each day we try to become more efficient and effective with our tasking. Unfortunately, we continuously hit roadblocks once we need to actually enter the system to carry out our tasking, and we leave our programs questioning our actual ability to carry out our objective, and support the warfighter.

Knowing that cyber-security measures are a large and growing focus in the DOD today, can it be determined that there is a correlation between the policy being implemented to mitigate cyber-security attacks and the efficiency of business and contracting productivity?

## A. BACKGROUND

SeaPort is a database of Multiple Award IDIQ contracts (MACs) awarded by NAVSEA to focus on strategic sourcing of Professional Support Services (PSS). SeaPort was developed by NAVSEA in large part due to the high volume of services procured each year. In addition to the high volume of service procurements, the Office of the Secretary of Defense (OSD) mandated fifty (50) percent of all support services be acquired through use of performance based contracting by 2005 (NAVSEA, 2001). Additionally, the Command was failing to capitalize on economies of scale without centralizing and coordinating requirements through a common contract vehicle (NAVSEA, 2001). SeaPort was developed to address each of these areas. By committing to using a centralized MAC, the Navy is now able to deliver faster, more effective, and more efficient service support to the programs and warfighter. SeaPort launched on April 2, 2001, allowing for business with over twenty (20) industry partners, through an electronic portal, on a World Wide Web website.

> The Naval Sea Systems Command (NAVSEA) procures over a half billion dollars of Professional Support Services (PSS) each year for its headquarters' Directorates, Program Executive Offices (PEOs), and field activities. In order to meet the Navy strategic sourcing wedge, NAVSEA committed to $250M in savings by procuring PSS more efficiently. Coupled with this need, the Office of the Secretary of Defense (OSD) directed that 50% of all support services be procured using performance based contracting by the year 2005. Furthermore, NAVSEA had more than 450 separate PSS contracts supporting its requirements. Most of these efforts were not integrated from a Command perspective, utilized a multitude of different processes in which to procure the services, and did not leverage corporate buying habits or e-business to facilitate the processes. In addition, the services were predominantly procured via level of effort vice performance-based terms. (NAVSEA, 2001, p. 1)

SeaPort is used by one-hundred twenty-one (121) government ordering activities with eight (8) commands. SeaPort works by streamlining the IDIQ processes allowing vendors to sign up for portal access which enables them to bid, administer, and monitor pre and post awards as well potential award opportunities. An IDIQ contract is one that provides an indefinite quantity of supplies or services during a specific period of time. Minimum and Maximum quantities are established within the contract. This type of contract is used when a specific number of supplies or services can be determined. This is especially useful in R&D type contract work. When a vendor is awarded a MAC (Multiple Award Contract) contract in SeaPort they are able to bid on potential services for potentially fifteen years. There are eight benefits and innovations according to SeaPort's FAQ page including benefits such as the potential for a fifteen (15) year contract, guaranteed savings clauses, focus on quality and a fully electronic Task Order system (NAVSEA, 2001). These benefits are important to the success of the overall SeaPort program and its ability to support the warfighter. Unfortunately, the first benefit describing the potential for a fifteen (15) year contract decreases the last two benefits focused on quality and a fully electronic system. In 2016, the system, which was brought online at the outset of the program, is fifteen (15) years old in an environment where technology, computers, and systems become outdated in two (2) years or less.

SeaPort is a MAC contract. A MAC contract is a multiple award contract used for SeaPort award procedures. When a vendor is awarded a MAC contract (which is an award to join SeaPort) an IDIQ number is assigned to that vendor. A Task Order number is assigned to their MAC number every time an award is made to that vendor. SeaPort was launched on April 2, 2001 with twenty-one vendors. On April 5, 2005, 151 were awarded a MAC contract. SeaPort now has more than 2400 vendor MACs.

According to SeaPort's security page, "Resources have been applied to assure information security commensurate with the risk associated with use of SeaPort for acquisition, collection, storage, and dissemination of information. The SeaPort portal uses the most secure commercially available 128-bit password-protected Secure Socket Layer (SSL) session encryption between the server and client as well as time/date stamping to provide evidence of intent on the part of buying and selling parties (i.e., an electronic

signature). It is incumbent on all users to protect their password appropriately" (NAVSEA, 2001, "Security"). SeaPort basically uses encryption technology along with CAC enabled security to ensure that unauthorized users cannot gain access to sensitive information. Information stored within SeaPort can hurt the warfighter but can also hurt private entities as they store and transfer propriety data such as cost and technical capabilities. SeaPort must have the best security features to protect U.S. interests. Secure Socket Layers or SSL works by allowing a user to encrypt information sent or received across a network and is useful in protecting data such as Personally Identifiable Information (PII), credit card information, and other sensitive information in general (Symantec, 2016).

SeaPort has "more than 570 SeaPort task orders set to expire in fiscal 2016, with a combined ceiling value of $13.3 billion, and an average of 3.6 of bids received per task — which could mean opportunity for both new and existing vendors" (Sakole, 2015, p. 18). The article written by Sakole of Deltek.com goes on to say how $30.3 billion has been spent over the last six years. With this kind of money and emphasis on the Warfighter, it is apparent that SeaPort is a special tool for the Navy and Defense. As worldwide tensions and conflict grow everyday it is important to understand that SeaPort is a major part of the backbone our Warfighters to ensure they get what they need to complete their mission, whether it being a service or material. It is understandable that SeaPort has the best security measures to protect sensitive and proprietary data. But does this mean we should have thick, heavy duty security protocols that slow down the system. What good is SeaPort if you can't use it to efficiently acquire goods and services?

## B. PURPOSE

In researching both cyber security and the relationship to SeaPort, we will attempt to answer the questions, "Is cyber security becoming too restrictive?" and "How can the DOD, specifically NAVSEA, do better?" Describing the cyber and SeaPort environments and answering the questions above will be bolstered by the research and analysis we complete. A discussion of that research and analysis will be provided to back up our ideas. In the end, the project should provide a summary of our findings and the

conclusions that were drawn from those findings. Those conclusions will include a recommendation for any business process or practice improvements that could be implemented to better support the DOD programs and warfighter.

Since most cyber-security information is classified and access is limited to individuals with specific need to know, our research will only scratch the surface of cyber security's effect on SeaPort. With that said, this research should lead to further research with a more in depth focus and additional cost benefit analysis of certain cyber-security measures in place today; especially with the growing need for more and more safety measures and protections around defense systems and secrets. By bringing the research topic to light, we hope to assist in finding the current problems with our support systems, specifically SeaPort, in order to make adjustments that will make our business and contracting practices more effective and efficient. As noted above, there will be cyber-security information we do not have access to, however, another benefit of our research will be to provide an overview and analysis of the actual effects of cyber-security policies we do have access to on business and contracting support effectiveness. Through a comparison of current business practices and policies to actual support being provided to DOD programs and ultimately the warfighter, we can present a link between the policies and security measures in place and the inefficiencies of the SeaPort system faced by Contracting personnel on a day-to-day basis.

## C. RESEARCH QUESTIONS

With the increased focus on cyber security, there are potential implications on business system performance and business productivity. Our research will focus on those implications and attempt to answer the following questions:

1. Is cyber security becoming too restrictive, making the ability to support the programs and warfighters inefficient and ineffective?

2. How can the DOD, specifically NAVSEA, do a better job of implementing cyber-security measures while conducting business in an effective and efficient manner?

3. What business practices could be put in place to protect the DOD without hindering contract and business support to the warfighter?

## D. SCOPE

The research team was tasked with identifying a viable topic for further research and analysis in order to better prepare the team for critically analyzing issues and finding resolution in day-to-day operations and that would provide better insight into and possible resolution for a very real and existing problem faced today in the DOD. The team initially consisted of the student researchers, Danielle Allen, Daniel Belcher, and Bill Turner, each an employee of the NAVSEA, NSWCDD Contracting field office. The team identified one of the largest issues plaguing the entire Contracting department at the NSWCDD, under performing and inefficient business systems required for everyday business activities. The team generated multiple hypotheses to potentially research and analyze throughout this project. We determined the most interesting and viable option based on current awareness of and priority placed on cyber security in the DOD.

The research team proposed the idea of a joint applied project, focused on cyber security, to the Principal Investigator who further assisted in scoping the topic into a more manageable field of study and research. The team began to shrink the vast topic of cyber security into an applicable topic of research and analysis of the cyber-security topic as it relates to systems being used by Contracting Officers and Contract Specialists across the NSWCDD and NAVSEA. The team agreed the topic of interest would involve a study of the effect of cyber-security measures being implemented in the DOD, and more specifically implemented within NAVSEA, on the effectiveness and efficiency of our support of program missions and the warfighter. The primary focus would be on the policies that are put in place on business systems and business practices that lead to ineffective and inefficient program and warfighter support. The goal was to identify and bring awareness to the problem and provide recommendations for solving the problem from a business policy and practice perspective.

## E. METHODOLOGY

The team began by discussing the research topic further amongst each other to assist in developing a pathway for the research and analysis to be performed. Since the research could easily become too technical for a research team not qualified with any

technical expertise, it was determined that focus of research would be on cyber-security policies, and therefore practices that are put in place to ensure compliance, and how it relates to performance capabilities of the teams expertise, supporting the Navy through Contracting. In order to provide a well-rounded discussion of the topic, the researchers determined the first steps forward would involve a brief overview and background of what the Internet, network, and computer systems are, and how they are interlinked. This overview was to be fundamental in nature to assist in an understanding of the interlinking of networked systems and how cyber security became necessary due to that interlinking of systems across the globe.

Research would then grow to be a more in depth look at policies and practices in place, and how they have actually been implemented, that affect the capabilities and speed of SeaPort, one of the most predominant systems used within the Contracting field at the NSWCDD. Research included gathering information through searches of Internet document repositories, published articles, government websites, and published policy on federal government intranet networks.

Further research plans included direct, random, and anonymous surveys of individuals across the Contracting competency at the NSWCDD. These individuals included Contract Specialist, Policy personnel, and Systems support at the NSWCDD who are day-to-day users of the SeaPort system. The individuals selected for the survey were selected at random from a list of all eighty (80) of the non-supervisory government employees in the Contracts department at the NSWCDD. No more than thirty (30) individuals were selected to participate in the survey and participation was voluntary. Data from the survey was analyzed to determine any patterns or similarities from the respondents. Responses were then placed into generalized groupings based on the patterns and similarities that were discovered in analysis, in order to maintain full anonymity of respondents.

Through compiling the fundamentals of the Internet and networked systems and associating the policies that were found through our research the team planned to draw connections between the threats associated with fully networked systems and the need for the policies that have been implemented by the cyber-security community within the

DOD and NAVSEA. Further, the analysis of survey data was then used to determine the effects of those policies on the daily operations and support of the Program and warfighter.

Based on the data and research collected by the research team, we plan to find a correlation between cyber-security implementation and draw a conclusion on the effect of cyber security on the ability to perform the duties of supporting the warfighter through providing contracting support. That conclusion of correlation between policies and actual system performance will be based directly on the analysis of research and data collected throughout this research. The recommendations for potential solutions to the performance issues of SeaPort will be drawn from experience in the business operations as Contract Specialist and will hopefully lead to awareness of the problem and more in depth research of the problem and recommended solution by individuals with technical expertise in systems engineering and development.

THIS PAGE INTENTIONALLY LEFT BLANK

# II. LITERATURE REVIEW

## A. GENERAL RESEARCH: GENERAL CYBER INFORMATION

*The Oxford Dictionary* (2016) defines a cyber threat as "a potential of a malicious attempt to damage or disrupt a computer network or system." It defines cyber crime as "criminal activity attempted by use of the Internet or some other computer network." As you can see from the two definitions, both cyber threats and cyber crimes are related. In many cases you cannot have one without the other. A cyber threat in and of itself is a cyber crime. Furthermore, a cyber crime can be perpetrated through use of a cyber threat. According to searchsecurity.com, "Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission (Rouse, n.d., p. 1). Rouse (n.d.) further discusses how the U.S. Department of Justice expands the definition of cyber-crime to include any illegal activity that uses a computer for the storage of evidence" p. 1). Cyber crimes are possible when the network responsible for the interconnection of computers have been compromised through an illegal, unauthorized intrusion of some form which opens the door for cyber incidents such as stalking, bullying, terrorism and identify theft (Rouse, n.d.).

Cyber crimes are often a result of a low risk, high reward situation. The unidentified authors at Cross Domain Solutions indicate "accessing sensitive information and data and using it means a rich harvest of returns and catching such criminals is difficult" (Cross Domain Solutions, n.d. p. 9). Cybercriminals are in it for the quick return, almost instant benefits. Like any other criminal, they steal, deceive and exploit people to get what they want; however, these types of crimes are committed behind a computer screen, usually where the criminal is nowhere near the victim (Cross Domain Solutions, n.d.). These types of crimes can be committed in different states as well as different countries.

There are many different types of cyber attacks that are defined as attempts at illegally obtaining control or access to an electronic device without the permission or knowledge of the owner. The illegal access poses a threat to the system and any

information stored therein. Cyber attacks are used to penetrate the security of an electronic and obtain any information stored therein (Sullivan, 2015). Cyber attacks happen daily in various different ways. Cyber attacks are when someone or something illegally accesses your digital device and has control of your digital device. There are over thirty different types of cyber attacks; those that are known to affect SeaPort performance and speed are listed and described below:

1. **Backdoors** – Unnoticed by the victim, this threat occurs when an attacker uses a back way into a system in order to install tracking software or other illegal tools granting unauthorized access to that system. A threat such as this becomes more serious than others as it gives an attacker the ability to unknowingly access, change, and control a computer system as well as obtain information from the system without authorization to do so (Sullivan, 2015).

2. **Denial-of-Service Attack (DOS)** – A form of attack that overwhelms a system or network by releasing a surge of traffic into the system inhibiting the ability of the device to connect to the network. Typical victims of this attack could include servers or websites of banks and credit card payment gateways due to the vulnerability of the data being transferred across this medium(Sullivan, 2015).

3. **Social Engineering** – An attack where an individual uses a small piece of knowledge to gain trust and leverage a relationship against their victim in order to gain access to additional information or to a whole network (Khanse, 2014).

4. **Malware** – Software that is implanted in a server or device in order to cause harm or damage to the system. Malware can also be used to perform unwanted actions within the system such as deletion of files or infecting of the system with more malicious software (Sullivan, 2015).

5. **Adware** – A natural looking advertisement or set of advertisements developed and released into a network or application that are in essence fake. These advertisements are designed to look real, but to infect computers with viruses (Sullivan, 2015).

6. **Bots** – An application that repetitively runs on its own in order to overwhelm a system or give the appearance of normal tasking. These applications are useful in setting up automatic DOS attacks (Khanse, 2014).

7. **Spyware** – Just as the name implies, this is software that runs in the background spying on the user without their knowledge (Khanse, 2014).

8. **Phishing** – Email or other direct attempts to obtain information that is required to access a system such as usernames and passwords (Sullivan, 2015).

9. **Password Attacks** – A direct attempt at stealing a user's password (Sullivan, 2015).

10. **Distributed Denial of Service (DDOS)** – An attempt at a more widespread DOS attack. Used to shut down an entire system of servers or network (Sullivan, 2015).

Anyone who uses the Internet is a potential victim of the cyber threats listed above, but some of the more sophisticated and complex types of attack methods that affect both private and public sectors include: Advanced Persistent Threat (APT); Distributed Denial of Service (DDOS); Cross-Platform Malware (CPM); Metamorphic and Polymorphic Malware; and Phishing (Mukaram, 2014).

Advanced Persistent Threat is achieved by methods that are concentrated and sophisticated. These attacks are coordinated and directed at a specific victim (Mukaram, 2014). An APT attempts to obtain unauthorized access to information that is sensitive in nature without being detected and leaving behind no trace of ever being there (Mukaram, 2014). APT's are a favorite approach used by attackers when conducting cyber attacks on corporations and intelligence espionage (Mukaram, 2014).

APT's are designed so that valuable, classified data can be stolen, without a trace, and have been successful in the past; even when used against the most prepared Information Technology (IT) companies in the U.S. and Europe (Mukaram, 2014). An APT cannot be stopped by a single technology or process. Traditional security methods are not effective against these threats. Many organizations leave themselves vulnerable to these types of attacks because they are not investing enough resources into cyber-security methods which are updated regularly as new threats are created. It is imperative that companies invest time and money into addressing these types of sophisticated attacks. Money and time spent to educate their cyber experts, increase the levels of cyber security,

and obtaining advanced skills in order to better detect and end an ongoing attack is necessary (Mukaram, 2014).

Distributed Denial of Service is a type of threat that instead of stealing information, hackers simply knock-off their victims (Mukaram, 2014). This method is extremely effective even though it is not as technically challenging (Mukaram, 2014). Typically, this approach floods a network with huge packages of data (Mukaram, 2014). As a result of the bombardment of data, valid requests become lost or the service becomes too slow to work (Mukaram, 2014). An Internet domain's accesses are blocked in a successful DDOS attack (Mukaram, 2014). These types of attacks do not impact an organizations computer system internally. Mukaram makes it clear that at the very least a company should incorporate basic level security principals into their system security to protect their financial processing and trading networks which are key infrastructures to the success of their business (2014)

Cross-Platform Malware is not exclusive to windows operating systems (Mukaram, 2014). Mukaram says "the economic incentive to build cross-platform malware for cyber criminals rises with the growing number of systems using different operating systems" (2014, p. 12). A growing number of systems therefore results in a higher amount of CPM attacks.

Metamorphic and Polymorphic Malware is a type of malware that replicates itself and is never the same as its most recent version because the coding is designed to always be different to avoid detection and prevention (Mukuram, 2014). This type of malware is one of the biggest threats to any organization due to its ability to be undetected. Even standard anti-virus programs cannot recognize the attack (Mukaram, 2014). Since this malware is always replicating while morphing into something new, it is very difficult to design and build, taking techniques that would require the most skilled cyber criminals to carry out. Businesses relying on open source web applications are more susceptible to Metamorphic and Polymorphic malware.

Phishing is typically done via email. Hackers tap into a person's email addresses to gain access to a more global contact list and send out emails to those in their contact

list or address book pretending to be the sender (Mukaram, 2014). The receiver unknowingly opens the email not realizing that the person's whose email address it came from was not the person who sent it (Mukuram, 2014).

Because of all of the cyber threats and cyber attacks described above, that are performed to attack others, it is vital that individuals, private industry, and the public sector protect themselves through implementation of cyber-security protocols.

As we discussed above, cyber security exists to protect anyone using computer networks and systems to store data, information, or conduct business. In a digital age, computer networks and systems touch most anyone in the developed nations of the world. Cyber security puts this information that, if found, makes individuals and especially the DOD vulnerable behind layers of security. For example, it could be as small as entering the password to your home computer to access its capabilities (NCI, 2015). Or it could be equated to the use of a safe deposit box at a brick and mortar bank that first stores the safe deposit box in a locked, steel safe that requires both a code and a biometric scan to enter, and then the box itself requires two different keys held by two different individuals in order to be opened.

There are ways one can protect their personal information as well as any company data or information. A lot of financial companies as well as other institutions such as medical companies offer text and email notifications regarding their accounts activities when suspicious activities are attempting to take place. One is able to verify if the activity is valid or invalid before "real" damage can be done to their accounts. Creating strong passwords for your accounts is a good way to ensure that you are not vulnerable to cyber attacks. A strong password consists of various capital and lower case letters, numbers and characters. NCI indicates it is also important that you use different passwords for every account and change your passwords every couple of months (NCI, 2015). Check your bank statements often for fraudulent transactions often. Make sure that all withdrawals and purchases match your records and if any are not valid, notify your bank of all discrepancies immediately (NCI, 2015). NCI further indicated that companies should move all important data and information to a cloud-based server (2015). These types of servers are in one location and are great for consolidating data and keeping it safe. All

employees should be trained to follow good cyber-security practices. This prevents vulnerabilities to the company. Trainings should be done on a regular basis. A cyber-security expert should be on staff (NCI, 2015). These employees can keep an organization's cyber-security systems up to date with the latest and greatest cyber-security software as well as keeping it safe from cyber threats (NCI, 2015). Just as the examples described above, cyber-security measures can be as poor and minimal as only requiring one password to access everything or be more secure such as requiring multiple layers of security to be brought down before having an ability to access the information or items protected by those security measures.

## B. PRIMARY RESEARCH: CYBER SECURITY AND THE GOVERNMENT

The Internet is a set of computers all over the world interconnected through a network of lines such as cables, telephone line, or satellite connections. While the Internet is the interconnection of computers across the world, the web or the World Wide Web is the actual information and services used by people on the network every day. The Internet links countries, both allies and enemies, to one another through the cyber world without having an actual link in the physical world. Individuals and nations are able to pass information across this cyber space with minimal limitation.

According to Andrews and the History Channel, the Internet began as a workable prototype in the late 1960s when the DOD funded a project to create ARPANET, or the Advanced Research Projects Agency Network (Andrews, 2013). Beginning as a DOD project, the Internet was originally only planned for use among a single network of multiple computers within the DOD. History.com continues to provide a timeline of the Internet, as many individuals know it, through growth in the 1970s, expansion in the 1980s, and ultimately the release to the world in the 1990s (Andrews, 2013).

In the 1970s scientists Robert Kahn and Vinton Cerf continued research into the Internet and developed the Transmission Control Protocol and Internet Protocol (TCP/ IP), or the first model for transmitting information through numerous networks and systems (Andrews, 2013). This was the beginning of growth of the Internet into what we use today.

History further reports that ARPANET adopted the research of the aforementioned scientists in January of 1983, when researchers started to build a "network of networks" (Andrews, 2013). This "network of networks" is the expansion from a single network of computers communicating together to multiple networks of computers communicating together to other interconnected computer systems and networks (Andrews, 2013).

In the early 90s, computer scientist Tim Berners-Lee invented the World Wide Web, which is the Internet as we most frequently use it today (Andrews, 2013). Most people confuse the World Wide Web with the Internet because the World Wide Web is the typical way of accessing and using information online through use of websites and clickable hyperlinks (Andrews, 2013). This was the beginning of the collection of information and data that is now accessible across the globe every day (Andrews, 2013).

The Internet is useful because the lack of regulation allows for every network to connect to every other network ("How it Works," 2016). These open standards' do exactly as one would expect; they allow any individual to create and transmit data and offer and sell products and services. The very thing that makes the Internet great, for anyone and everyone, also makes it and its users extremely vulnerable. The openness of the Internet stems from the non-existence of a central authority reigning over the web. Also noted by internetsociety.org, the lack of a central authority allows everyone to communicate, produce, and compete on the same level plane (2016). Because of the interconnection of the world through a set of networks that are built to communicate with one another with no central authority and an open set of standards, any individual on the network is vulnerable to threats, attacks, and theft of their data that is available on the network ("How it works," 2016). This openness makes it more important to focus time and effort on cyber-security measures as the world becomes more technologically advanced and connected ("How it works," 2016).

The University of Maryland University College (UMUC) describes cyber security, also known as information technology security, as how users protect information that is passed across a network, or stored online, from being obtained, accessed, or changed without permission (UMUC, 2016).

UMUC indicates, “Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers” (2016, p. 3). Due to the high volume of data, both confidential and classified, that is stored and available in cyber space there is a clear growing concern for the safety and protection of that data (UMUC, 2016). This requires persistent and continuing awareness and attention to protecting sensitive data. Without focusing time, money, and manpower on protecting this information, businesses, individuals, and national security are all at a greater risk (UMUC, 2016).

Due to this growing risk, a Senate hearing was held in March 2013 where top intelligence officials of the United States warned that “cyber-attacks and digital spying are the top threat to national security, eclipsing terrorism” (UMUC, 2016, p. 4).

According to Caitlin Hayden, a spokeswoman for the Whitehouse National Security Council, “Cyber threats cover a wide range of malicious activity that can occur through cyber space” in an email that was sent to “The Verge”: “Such threats include website defacement, espionage, theft of intellectual property, denial of service attacks, and destructive malware” (“Broad Definition,” 2013, p. 3). Cyber threats are the main reason cyber security is becoming a necessary focus of individuals, private industry, and the DOD. The increased use of computer networks and systems, due to enhancements in technology, put enemies on a new playing field, where their attacks can be malicious and deadly without carrying out a physical plan of harm as we see with other terrorist attacks. Since cyber threats are malicious in nature and an attempt to damage or disrupt another user’s computer system, it is a form of cyber crime.

Based on a report from the Consumer News and Business Channel (CNBC) in September of 2015, the United States government budgeted $14 billion for cyber-security measures in fiscal year 2016 (Bukszpan, 2015). The Department of Homeland Security (DHS) plays an important part in protecting the federal civilian networks and cyber infrastructures necessary for the workforce’s professional and personal lives: “DHS’s National Cyber-Security and Communications Integration Center (NCCIC) is a 24x7 center responsible for the production of a common operating picture for cyber and

communications across the federal, state, and local government, intelligence and law enforcement communities and the private sector" (Homeland Security, 2016, p. 2). It is apparent that the federal government is taking seriously the cyber threats and cyber crimes that could be committed against the United States. This funding will be used to stiffen cyber security's role in deterring these threats and protecting the United States through finding and adding new layers of security to an already compartmented and protected system (Bukszpan, 2015).

A strategy among many other strategies that the president outlines in his 2016 Cybersecurity National Action Plan includes, "requiring agencies to identify and prioritize their highest value and most at-risk IT assets and then take additional concrete steps to improve their security" (Office of Press Secretary, 2016, p. 18). As a part of the Cybersecurity Act of 2015 the Obama administration is devoted to making cyber security a top priority to the country's national security initiative. Another point of the National Action Plan to note is that, "The Department of Homeland Security, the General Services Administration, and other Federal agencies will increase the availability of government-wide shared services for IT and cyber security, with the goal of taking each individual agency out of the business of building, owning, and operating their own IT when more efficient, effective, and secure options are available, as well as ensuring that individual agencies are not left on their own to defend themselves against the most sophisticated threats. The President's 2017 Budget supports all Federal civilian agencies adopting these capabilities" (2016, p. 20). The last important piece of information to note about the White House's National Action Plan is that $19 billion will be allocated to cyber security in 2017 which is a thirty-five (35) percent increase to the 2016 levels (2016). What specific cyber-security measures will be implemented? What is the DOD's strategy? What is the Navy's strategy?

A thirty-three page document entitled The Department of Defense Cyber Strategy is a document approved by Ashton Carter explaining the need to focus on America's security involving cyber related issues. The article goes on to describe three primary missions the U.S. Defense Department is focusing on to strengthen the cyber-security realm.

Carter says that mission one is to "defend its own network, systems, and information." The U.S. military's dependence on cyber space for its operations led the Secretary of Defense in 2011 to declare cyber space as an operational domain for purposes of organizing, training, and equipping U.S. military forces. The Defense Department must be able to secure its own networks against attack and recover quickly if security measures fail. To this end, the DOD conducts network defense operations on an ongoing basis to securely operate the Department of Defense Information Network (DoDIN). If and when the DOD detects indications of hostile activity within its networks, the DOD has quick-response capabilities to close or mitigate vulnerabilities and secure its networks and systems. Network defense operations on DOD networks constitute the vast majority of the DOD's operations in cyber space" (Carter, 2015, p. 12).

Mission two from Carter is to defend the U.S. and any interests to the U.S. against cyber attacks (Carter, 2015). Mission three is the counter measures against those cyber attacks (2015). Further in the document lists the next strategic goal which notes that Carter understands the DOD cannot protect against every threat to every network in use within the DOD, but does still need to find, analyze, prioritize, and defend the most important systems effectively (2015). Carter indicates it is also important that the DOD prepare for the worst case scenario that a cyber attack succeeds in order to ensure operations do not come to a halt when contingency operations are necessary (2015).

Finally, Carter explains that, "the DOD must raise the bar on technology and innovation to stay ahead of the threat by enhancing its cyber defense capabilities, including by building and employing a more defendable network architecture in the Joint Information Environment (JIE)" (Carter 2015). Additionally, he emphasizes the importance of the DOD coordinating and cooperating with the private sector to ensure defense data is protected and secure against detrimental cyber attacks (Carter, 2015).

A 2015 article published by the Office of the Deputy of Chief of Naval Operations for Information Dominance Navy Cybersecurity Division discusses how cyber threats are a critical threat to all aspects of the Navy's mission. The threats go beyond the traditional threats of just IT systems. "Machinery control, weapons, and navigation systems are now considered vulnerable as well as the networks and computers

commonly used by Navy personnel" (Deputy CNO, 2015, p. 1). The article goes on to talk about the newly established Task Force Cyber Awakening (TFCA) developed "to help improve the networks ability to defend against cyber attacks" (2015). TFCA reviewed hundreds of funding request that resulted in $300 million being allocated to FY16 to help defend and improve the Navy's IT defense. One priority for the Navy was for "control points" which acts in the same manner as a ships water tight compartment (Deputy CNO, 2015). If one part of the ship is flooded then it would lock down the area in order to not flood the entire ship. This helps to ensure if one IT area is hacked, the other parts of defense would not be affected. Can these implemented cyber-security measures slow down or affect system performance on the DOD systems such as the contract writing system SeaPort?

According to John Edwards and Eve Keiser of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), "Powerful and innovative security measures such as multifactor authentication and biometrics, along with strategic security planning and training could make launching attacks on DOD resources time-consuming and futile" (Edwards, 2015, p. 1). Finding specific cyber measures that are used for Navy Marine Corp Internet (NMCI) systems are most likely classified but other cyber-measure practices are described generally in C4ISRs. John and Eve describe multifunction authentication (MFA) in one part of their article in relation to the DOD cyber-security measures (2015). MFA is used "to help reduce exposure caused by phishing campaigns and login compromise, said Steve Orrin, federal chief technologist for Intel" (Edwards, 2015, p. 7). Orrin also recommended that "agencies consider augmenting MFA with contextual security controls such as location, device identity, device trust attestation and network access point" (Edwards, 2015)

A recent article written by National Broadcasting Company (NBC) News revealed that according to Security Scorecard, government cyber security ranked last place among 17 leading private organizations in the area of cyber-security strength (Reuters, 2016). Software patches, malware and network security were the poorest due to the large size of the government. National Astronautics and Space Administration (NASA) was the worst-rated government agency on these issues (Reuters, 2016). Massachusetts Institute of

Technology (MIT) says that software patches should be applied even if our computer and software is running fine. Software patches help strengthen your system and protect against malware ("Software patches and OS updates," n.d.). How many patches are used to support the SeaPort software? Do patches lower inefficiencies or slow down software? According to Brown (2016) at CIO Dive, 851 million records have been exposed over the last ten (10) years with 57.4 government employees and military personnel having their Social Security numbers stolen since 2005. This data can create a preliminary theory to suggest that maybe the DOD is overusing cyber-security protocols to fight cyber attacks. A look into cyber-security policies and procedures involving SeaPort could reveal over use of software patches.

## C. SECONDARY RESEARCH: CYBER SECURITY AND PRIVATE INDUSTRY

One of the larger aspects of cyber security and the implementation of particular protections to electronic systems is the actual effect on operational effectiveness and efficiencies. A blog posting from Executive Greg Day (2015) at FireEye, a leading cyber-security company against malware and advanced cyber threats, on FireEye's website indicates that roughly 37 percent of organizations receive 10,000 events per month tracked by cyber-security software. With the increasing number of events, or cyber incidents, companies spend more and more time attempting to identify advanced attacks before they occur, which is a difficult, intricate, and time-consuming process. The blog post further describes the process as ineffective since their data shows 52 percent of these incidents are false positives, leaving companies with making a judgment call on whether or not a threat of attack is reasonable and actionable (Day, 2015). The blog post from April of 2015 essentially sums up the unpredictable nature of cyber threats and the human error that plays into inefficiency and ineffectiveness of protecting computer systems and networks from advanced and malicious cyber attacks.

The company executive indicates the ideal situation would be to remove the guess work of determining a threat as real and focusing on responding to those that are (Day, 2015). The change in process would take the human involvement away from the forensic analysis of the threat by using a system that gathers all of the data pertaining to the

potential attack to determine whether or not it is real, so that the cyber-security team can focus on responding and eliminating the threat all together. The big point made in this article is that automating the process of determining the who, what, when, where, and why of a cyber threat or attack will allow the leveraging of technology to reduce the time and cost it takes to resolve the issue so that real day-to-day tasking of operations can receive full time and attention and actual work can be performed (Day, 2015).

More review on the topic of operational effectiveness as a result of cyber-security implementation led to an online transcript of a cyber-security video lesson provided by an Application Security Expert, Michael Cobb. Cobb, the founder and director of Cobweb Applications Ltd. of the United Kingdom, provides and overview of application protections and the balancing of security and actual performance.

In the lesson, Cobb (2009) speaks about the seven layers of the network and its security, beginning with the first layers, such as physical layers including switches and architecture. The next two layers of a system include network and transport such as routing devices (Cobb, 2009). All four of these system layers are protected by firewalls and intrusion detection systems (Cobb, 2009). And finally, Cobb touches on the final three layers, session, presentation, and application. While Cobb focuses on the application layer, he does indicate that a complete approach is the best functional way to protect a system. Cobb's focus specifically on the application layer is warranted as Cobb expresses the most important layer for protection is the application layer since seventy-five (75) percent of attacks now take place at that layer. Unfortunately, the lesson does indicate that application layer firewalls, used at layer seven of an infrastructure require processing power, which can result in reduced performance.

Cobb (2009) makes a point in his lesson that once an organization has implemented a security infrastructure at each layer of a network, performance comes into question. In a network as large as the DOD, and more specifically the Navy, the question becomes how well is the system actually serving the users and have you created bottlenecks by installing all of these security devices. Cobb goes further in his overview to indicate that the perception of the systems usefulness is just as important as what the actual data is showing. To summarize his expert thoughts, there comes a point where a

system becomes useless when a network infrastructure is overly restrictive (Cobb, 2009). He understands that blocking everything, such as email traffic, will ensure one-hundred (100) percent protection against email threats, but further describes that business as we know it would therefore come to a halt.

Cobb (2009) recommends as part of the security structure to implement smart, efficient security measures. This recommendation is not necessarily to increase Random Access Memory (RAM) or server size, which he notes could solve the problem but is not cost effective. Rather, he indicates adding load balancing devices such as content switches to the network will allow data loads to be shared across multiple services and reduce or eliminate bottlenecks of information passed to and from a centralized server.

After reviewing Cobb's overview of the balance between security and performance, we further dove into the effects of cyber security on performance. An article from AV-Test, an Independent IT-Security Institute, outlines an endurance test they performed to answer the following question: "Does anti-virus software slow down PCs?"

The article documents the process it took to obtain test results, which included seven (7) test rounds over fourteen (14) months of twenty-three (23) anti-virus products. The tests measured speeds of five different operations typically run by an end-user: downloading files from the Internet, launching websites, installing applications, opening applications (including a file), and copying files (Selinger, 2015).

The results of the test indicated no product obtained a perfect score and scoring ranged from 5.1 to 13.9 (Selinger, 2015). The potential range is 5–25, with 5 being the best possible score and 25 being the worst. To better illustrate the meaning behind these scores, AV-Test provides an example of two individual scores. A system with absolutely no protection takes 141 seconds to copy of the test file containing 3.3 Gigabytes (GBs) of data (Selinger, 2015). The same Windows system with the best performing system score based on the test required 165 seconds to download the same file (Selinger, 2015). Lastly, the security system on the same Windows system with the worst performing

system score based on the test required 300 seconds to download the same file (Selinger, 2015).

Ultimately, the article from www.av-test.org determines through its tests that good security software does not slow down a computer (Selinger, 2015). The emphasis, however, is on the idea that the security software must fall into the 'good' category based on AV-Test's speed test. They also note that it is apparent that other security software systems are in fact less efficient in performing typical computer tasks and sometimes run 2.5 to 3 times as slow as an unprotected computer or computer protected with the best performing software (Selinger, 2015).

Another resource identified in our research includes an online buying guide provided by a team of Information Technology (IT) professionals and editors, which produces product reviews, news analysis, and case studies focused around vital technology segments such as cloud computing, software and services, networking, and information security (cyber security) (Isaacson, 2014). The IT Pros team analyzed and walked through a book, "Understanding Big Data Scalability" discussing scaling applications and the fundamentals of application scalability (2014). The article discusses scalability, or in the terms of IT, the ability of an IT infrastructure to support networking through increasing or decreasing the size, or number of servers required in a given time period and operational volume (Isaacson, 2014).

The article presents the goals of a scalable application or platform as being able to provide an organization with adequate networking support and capability without sacrificing efficiency and effectiveness (Isaacson, 2014). In essence, the IT expert indicates an automated scaling up and down of the capability is ideal as demand for a server's performance has peaks and troughs (Isaacson, 2014).

The author further describes the requirement of an application to be capable of spreading the load of work across multiple servers as an application with high volume of usage will eventually meet the limits of a single server (Isaacson, 2014). The options to resolve this problem based on the author, Cory Isaacson's, Chief Executive Officer

(CEO) of CodeFutures Corporation, experience and research is to either scale up or scale outward (2014).

As previously discussed in the review of the article from Michael Cobb, scaling upward or scaling outward are not the only options, but based on Cory Isaacson's review when we are discussing 'Big Data', scaling up or outward may be the only option since the volume of data is so large and the memory available for processing the data is limited by the size of or number of servers available on the network (2014). Scaling up is the process of buying a new, larger system, while scaling outward is the process of buying additional servers then distributing the workload across those servers as the volume requires (Isaacson, 2014). Ultimately, the author identifies these two possible solutions for performance issues tied to limited server availability (Isaacson, 2014). Within those solutions, there is a caveat that as you increase the scale of your applications with additional or larger servers, you open up the architecture to more points of failure (Isaacson, 2014).

The review of information pertaining to networking and cyber security available from the private sector, to include businesses, CEOs, and other IT experts outside of the federal government, gives an insight into how networking, servers, and cyber security are connected. Analysis of this information will provide a better insight into exactly how all of this information is connected and how it is linked to the poor performance of the government contracting system, SeaPort.

## D. SUMMARY

The above literature discussing the Government's stance on cyber security shows the determination of the White House to implement cyber-security measures for the DOD and the U.S. Spending thirty-five (35) percent more of the FY17 budget and putting new programs in place is just a couple of ways cyber security is being tackled. A very important point to keep in mind is quality vs. quantity. The White House is enacting mass security measure rapidly instead of gradually implementing policies and program (Office of Press Secretary, 2016). With this come inefficiencies that can happen due to over saturating the Defense cyber world with firewalls and authentication protocols. Is this

why government and Defense systems have become inefficient and slow? This is a preliminary theory that can be the result of the new aggressive push for cyber-security measures. This combined with analysis of random survey of experienced users of SeaPort, the Navy's contract writing system, can help lead this research into finding out if cyber security is causing inefficiencies in SeaPort.

Through reviewing the literature available from the private industry, it is apparent there is a problem with determining and keeping track of actionable and real cyber threats. Based on the information provided in the FireEye article, we can estimate that over 47.6 billion cyber incidents occurred monthly among non-governmental organizations, in the United States alone, in 2012. This data is based on thirty-seven (37) percent of the 12.89 million entities reported in the 2012 Economic Census, conducted by the United States Census Bureau, receiving ten-thousand (10,000) incidents per month. It should be noted that the ten-thousand (10,000) incidents per month FireEye identifies is based on incidents tracked through cyber-security software. This does not account for those incidents that are not identified by cyber-security software because the organization does not utilize such software. Because the Census Bureau data does not account for governmental organizations in the available 2012 Economic Census data and the ten-thousand (10,000) incidents per month could actually be low since not all organizations utilize a cyber-security software, it is plausible that many more incidents occur than the estimated 47.6 billion. (All Sectors: Core Business Statistics Series: Advanced Summary Statistics for the U.S. (2012 NAICS Basis): 2012, 2014) Based on the statistic and information above, it is easy to see why cyber attacks and cyber threats are such a problem. But a deeper issue, still, is the other statistic provided by FireEye. Fifty-two (52) percent of those estimated 47.6 billion incidents per month are false positives and not actually a real, actionable concern. This means that 24.75 billion incidents, in the United States, per month are nothing more than a false reading. While that still leaves 22.85 billion incidents that must be addressed, the failure rate is like flipping a coin and losing, or making the wrong call, more than half of the time. The biggest concern is that, just as the article from FireEye states, these determinations to pursue a threat are left to human judgment.

Applying the same information, we can produce an educated estimate of the number of cyber incidents that occur across the one-hundred twenty-one (121) government ordering activities that utilize SeaPort for the procurement of service support. If we assume thirty-seven (37) percent of the organizations see ten-thousand (10,000) incidents per month, then roughly 447,700 incidents should be tracked through their systems, by their cyber-security software, on a monthly basis. It is clear to see that the sheer number of incidents mixed with human processing and error lead to inefficient, ineffective, and poorly protected systems.

A deeper look at the data obtained by AV Test in its independent study of twenty-three (23) anti-virus products, a standard cyber-security measure, shows a significant association between the use of an anti-virus software product and the processing speed of a computer or network. A system with no anti-virus software can copy a file at speeds of about 42.7 seconds per GB. That same system with the best performing anti-virus software would average speeds of about 50 seconds per GB, and the worst-performing anti-virus software would average speeds of about 90.9 seconds per GB to copy a file. This has major implications on the type of anti-virus software one introduces into a computer system or network. Information such as this should be taken into account when determining the importance of one's work and the required efficiency levels of one's organization. In a high-volume organization, processing high numbers of procurement actions and with shortened timelines to meet milestones, the difference between the best quality anti-virus software and the lowest quality software is more than trivial. When processing times begin to double due to anti-virus software, which is only one layer of security in a cyber-security system, efficiency may begin to suffer.

# III. DATA AND ANALYSIS

## A. DATA/SURVEY

Thirty (30) Contract Specialists were randomly selected from an alphabetical list of eighty (80) employees in the Contracting field at the NSWCDD. Of the thirty (30), sixteen (16) Contract Specialists from Dahlgren chose to participate in the SeaPort study regarding latency, slowness, and other issues that caused inefficiencies with the contract writing system by responding to the survey. The sample size of sixteen (16) Contract Specialists represents twenty (20) percent of the NSWCDD Contract's department population.

The survey was designed to obtain information pertaining to user level experience of the SeaPort contract writing system. The population was selected because the system is only as effective and efficient as it is perceived to be by its users.

### 1. Data Set 1: Key Issues SeaPort

Question one (1) of the survey focused on key issues contract specialists are confronted with when using the contract writing system in performing their job duties. Twelve (12) out of sixteen (16) participants, or seventy-five (75) percent, that were surveyed said that Seaport performed poorly or did not perform at all when attempting to connect for generation of Federal Procurement Data System-Next Generation Contract Action Reports (FPDS-NG CAR). Twelve (12) out of sixteen (16) participants also indicated Seaport did not perform when generating Portable Document Format (PDF) solicitation, award, and modification documents. Seven (7) out of sixteen (16), or almost forty-four (44) percent, of participants indicated they could not get a line of accounting to load once the funding was received in SeaPort. Twelve (12) out of sixteen (16) participants experienced overall latency in toggling between different windows within the system. See Figure 1 for a depiction of the data. One participant said that Seaport in general is "Slow, unpredictable, time consuming, frustrating, and always has issues." One-Hundred (100) percent of the participants commented on the SeaPort system's reliability concerning completing tasks such as incremental funding modifications,

adding lines of accounting and in general speed and latency. This survey question provides evidence that SeaPort has issues which effect performance and efficiency.

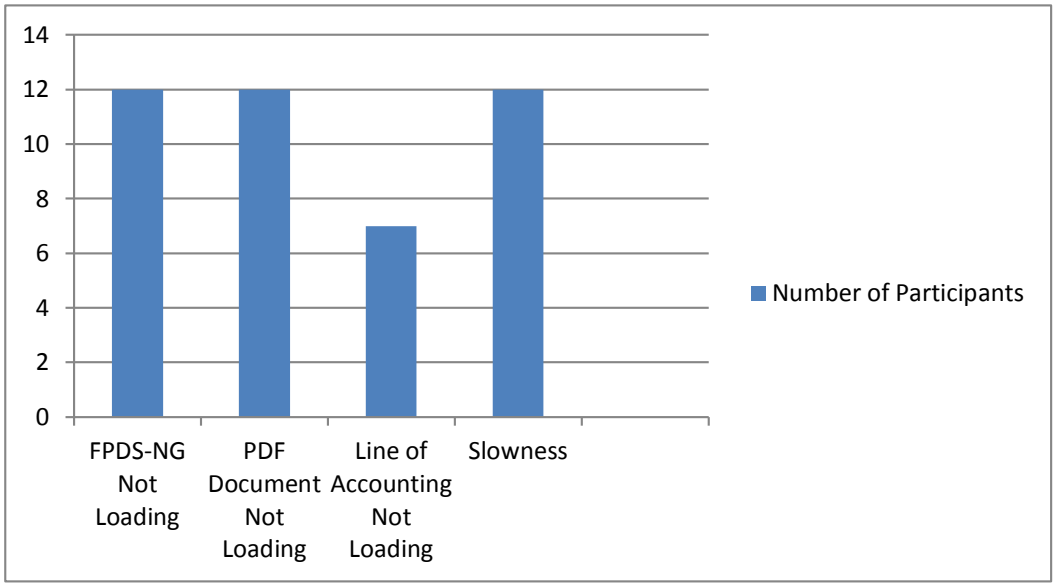


Figure 1. Main Issues Identified with SeaPort

### 2. Data Set 2: Submission of Help Desk Tickets

To further reinforce the data collected in question one, the participants were asked to comment on their use of the SeaPort Help Desk. Fifteen (15) of the sixteen (16) participants, or ninety-three (93) percent, stated that they submitted Help Desk tickets related to the connectivity for generating FPDS-NG CARs, generation of PDF solicitation, award, and modification documents, and general system speed and latency issues. Figure 2 shows the number of SeaPort Help Desk tickets submitted by specific issue.

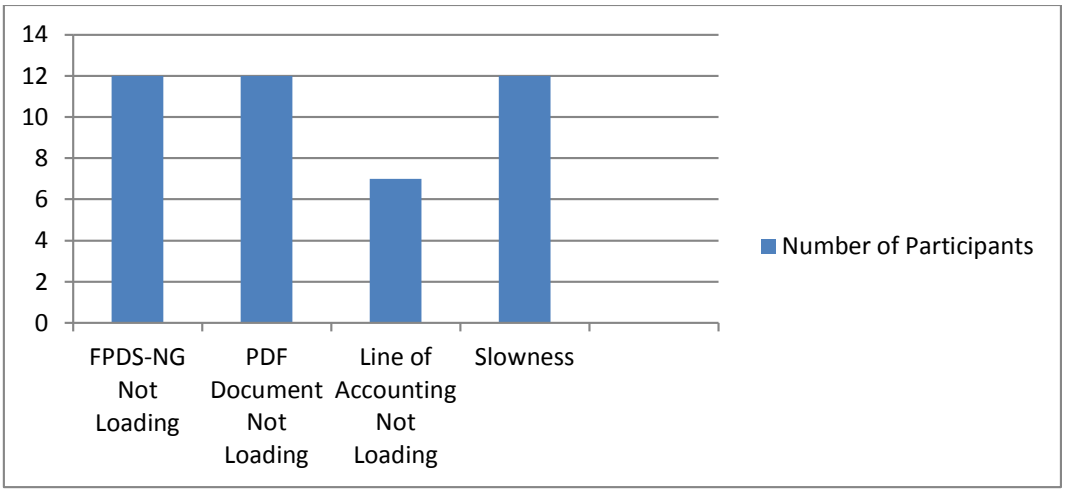


Figure 2. SeaPort Help Desk Tickets Submitted by Survey Participants

The data presented in the Figure above is a depiction of the actual results of the survey. Although fifteen (15) of the sixteen (16) participants stated they submitted a Help Desk ticket, due to the format of data collection, not all fifteen (15) submitted tickets for the same exact issue. The Figure above represents the number of tickets submitted by individuals related to each issue. Some individuals reported submitting multiple tickets as a result of facing multiple issues.

### 3. Data Set 3: Frequency of Issues

The next survey question was designed to provide a snapshot of the current environment of the system and focused on the frequency of issues plaguing the systems performance in the recent past. All sixteen (16), or one-hundred (100) percent of participants, said that SeaPort had issues pertaining to generation of FPDS-NG, generation of PDF solicitation, award, and modification documents, and latency issues over the last six months of use. Latency issues include inability to produce incremental funding modifications or add lines of accounting within the system.

### 4. Data Set 4: SeaPort Use

In order to provide insight into the importance of the system to completing responsibilities as a user and to draw attention to the amount of time attempting produce

work within Seaport. Of those who participated in the survey, half of respondents indicated they spent more than four (4) hours in Seaport daily. Eleven (11) of all sixteen (16) participants indicated that three (3) or more hours out of their workday was spent in Seaport. This equates to nearly half of a full, regular working day in Seaport, one of many business systems in use by contracts. Figure 3 shows an even split in terms of amount of time spend by individuals in the SeaPort system.

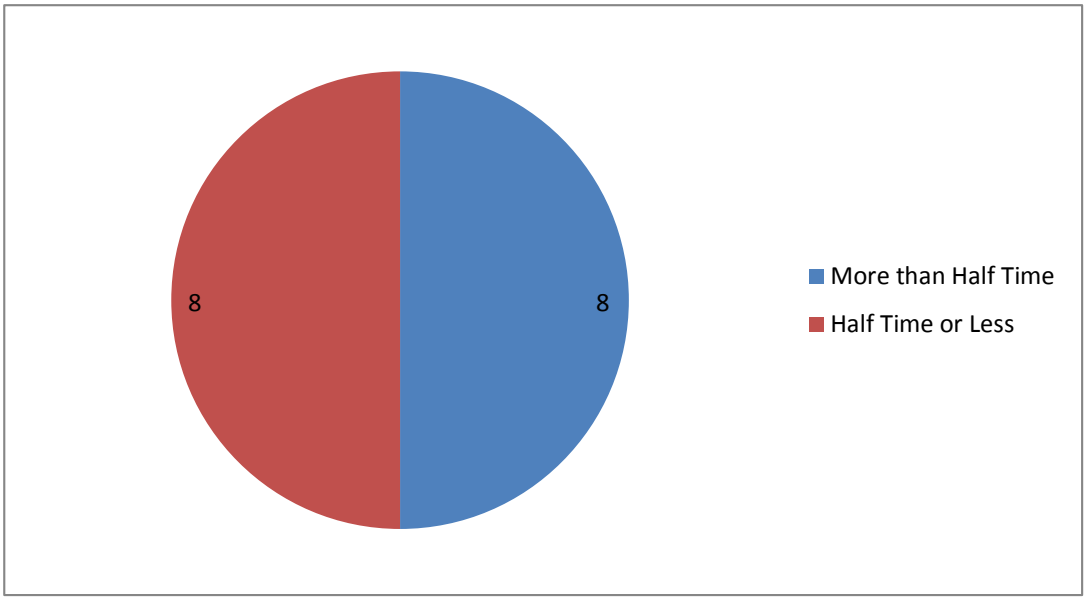


Figure 3. Amount of Time Respondents Spend in SeaPort

### 5. Data Set 5: SeaPort-e Help Desk Ticket Time

The last question pertaining to Seaport was in regards to the responsiveness of a completely automated Help Desk. Of the sixteen (16) participants, fifteen (15) indicated they submitted Help Desk tickets. Almost seventy-four (74) percent of those fifteen (15) indicated they waited more than one week to get a response from the Help Desk. As shown in Figure 4, nine (9) of those individuals waited two weeks or more for a response. With one-hundred (100) percent of participants facing at least one performance issue warranting the submission of a Help Desk ticket over the last six (6) months, and ninety-three (93) percent of those users actually submitting a Help Desk ticket it is possible the

system has been flooded with too many tickets further slowing the bandwidth of the system.

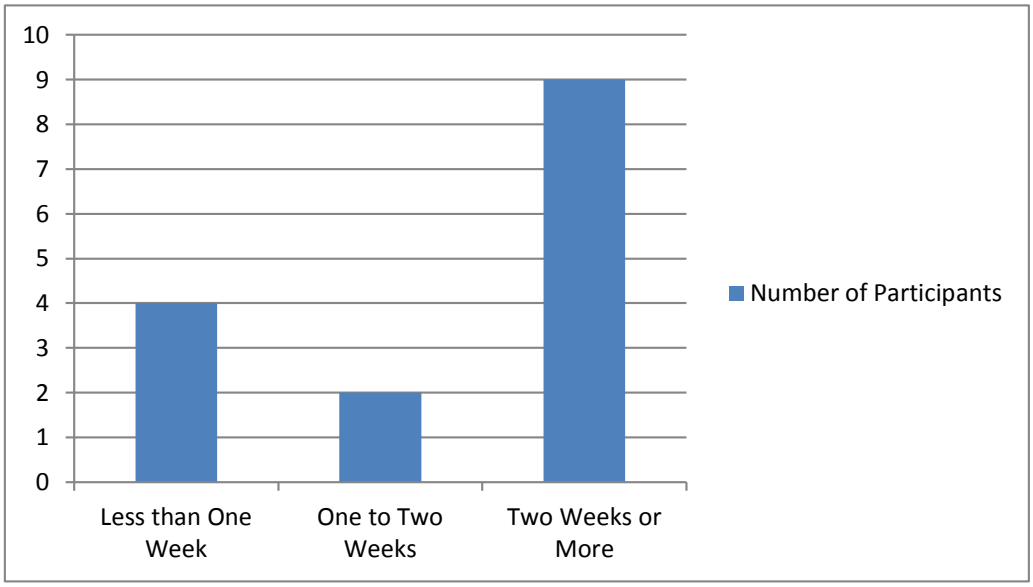


Figure 4. SeaPort Help Desk Response Time to Submitted Help Desk Tickets

## B. DISCUSSION ANALYSIS

With the survey design set up to obtain information at a user level, in order to provide a better insight into the day-to-day operation of the SeaPort system, we specifically focus on errors and issues any user could see at any time. Also, the limitation on access to non-anecdotal data due to restrictions and limitations on the availability of that tangible cyber-security data we are limited to discussing day-to-day issues that arise at the user's level.

The data received shows evidence that SeaPort is in fact afflicted with issues that slow down productivity in administering and executing contracts; contracts which directly affect the performance of programs that support the Navy's ships and warfighter. These issues include extreme latency and non-responsiveness, nonfunctioning interfaces, in ability to generate solicitation, award, modification, and reporting documents.

Based on the data we collected at NSWCDD, if we apply that information to SeaPort at large, we can use it to determine the potential effects an under-performing system has on a Contract Specialist's ability to provide contract support to a program and ultimately the warfighter. If we assume that at the one-hundred twenty-one (121) government activities using the system across eight (8) commands, an average of 20 Contract Specialist uses SeaPort at each activity, we have over two-thousand (2,000) Contract Specialists alone using the system at any given time. This estimate is conservative considering the NSWCDD is one of the smaller field activities within NAVSEA and has eighty (80) Contract Specialists. It should also be noted that there are over 2,400 IDIQ MAC holders in private industry, along with government Contracting Officer's Representatives (CORs) and technical Subject Matter Experts (SME) who have access to the system at each field activity too. Based on the number of government users and companies that have access to the system, there is the opportunity for over twenty-thousand (20,000) individuals to be accessing the one server that operates SeaPort at one time. In addition to that, if ninety-three (93) percent of those users encounter issues within the system that result in at least one (1) submitted Help Desk ticket then the Help Desk is processing at least 18,600 tickets.

The fact that the Help Desk, in most cases, takes over two (2) weeks to respond to a Help Desk ticket means the backlog continues to grow and the Help Desk cannot keep up with processing tickets. These tickets include generating PDF solicitation, award, and modification documents which are required in order to initiate performance under a contract from a Contractor, correcting connectivity issues with FPDS-NG, addressing the speed and latency issues the users are encountering, and other performance issues that are being reported. The other important information to take into account is the data requested in the surveys intentionally left out other issues that would cause a Help Desk ticket to be submitted that would not be associated with an overly restrictive cyber-security measure such as a simple password reset, a request for system access, or a request for account unlock or reactivation due to inactivity of the account.

The two (2) week delay in response to correct an issue holding up a contract action itself is an unproductive, inefficient, and ineffective business process that effects

support to the warfighter. However, when you add in the fact that many of these issues can be tied to SeaPort's use of a single server and bottlenecking of bandwidth, which both may be cyber-security measures implemented to ensure system access and usage is for official business, by official, authorized personnel, and within the guidelines of network usage requirements. Another potential implication of the long lead time on responses to Help Desk tickets is the Help Desk's inability to correct the actual problem due to cyber-security requirements. This inability to correct the problem is not associated with the lack of technical capability, rather with the lack of authority to make the proper corrections to the system to incorporate the change.

## C. SUMMARY

Although the data is anecdotal and lacks the complete objectivity of a numerical rating scale or hard data from a reporting system within SeaPort, it does provide a snapshot of the user level effects of a poorly performing system. When, based on the data, half a workday is spent in SeaPort and most likely during that time in SeaPort an individual is encountering and attempting to work through system issues, the DOD is suffering a loss of productivity, efficiency, and effectiveness.

If one hundred (100) percent of an organization is spending half of their workday addressing a problem with the technology that is supposed to be designed to help conduct their job duties, then that organization is losing its ability to effectively support the warfighters mission. Addressing these problems rather than completing the actual duties of a Contract Specialist, which is putting money on contracts to fulfill program requirements and provide the ships and warfighter with the maintenance, training, and equipment they need.

THIS PAGE INTENTIONALLY LEFT BLANK

# IV. FINDINGS/RESULTS

## A. PRIMARY RESEARCH FINDINGS

Primary research findings were revealed in the data analysis and led to the fact that SeaPort has performance issues with generating PDF documents, FPDS-NG reports, line of accounting errors, and overall SeaPort latency. This finding was a huge milestone in understanding the "what" factor of SeaPort issues. The data analysis captured this information in sixteen (16) SeaPort surveys. The collected data further supports the idea that there is some form of bottlenecking, limited bandwidth, or poorly designed system infrastructure that causes inefficiencies. These inefficiencies include limited and reduced ability to award and fund critical support contracts for the DOD programs that directly arm and support our warfighters.

## B. SECONDARY RESEARCH FINDINGS

Unfortunately, due to the sensitivity of cyber-security measures and classified information, it cannot be determined if cyber security is the main culprit or if it has anything to do with SeaPort issues. Even though we could not find a direct correlation between SeaPort and cyber security, we can still hypothesize that cyber security plays a role in generating issues and latency of SeaPort. According to the secondary literature review above we can look at Cobb's focus on the seven layers of cyber security, specifically on the application layer and make a hypothesis that the application layer firewalls, used at layer seven of an infrastructure require processing power, can result in reduced performance.

## C. SUMMARY

To summarize the findings, it can be said that PDF Documents, FPDS-NG reports, line of accounting errors, and overall SeaPort latency were the issues that SeaPort users continually experience, according to the SeaPort users on the floor. Following the survey, we used literature to form a link on how SeaPort could be having issues due to cyber-security measures.

THIS PAGE INTENTIONALLY LEFT BLANK

# V. CONCLUSIONS, RECOMMENDATIONS, SUMMARY AND AREAS FOR FURTHER RESEARCH

## A. CONCLUSIONS AND RECOMMENDATIONS

In conclusion, this study defines what SeaPort does for the Navy, what cyber security is, and how it plays a role in the government sector as well as the private sector. Literature Review was obtained from studies done by Bukszpan on the government sector and Cobb on his studies of cyber security on the private sector. Data analysis was created by using survey questions directly distributed to sixteen (16) SeaPort users in order to find out factually what issues SeaPort was having. Recommendations can be made to help alleviate some or all of the issues related to SeaPort document generation, line of accounting issues, and latency. The following are recommendations that could be implemented business-wide.

1. If bottlenecks are occurring due to cyber-security measures that limit the number of servers a system uses in order to reduce the potential for a successful cyber attack then a more effective way of protecting the system should be designed and implemented that better positions the DOD to protect its servers while efficiently supporting the warfighter. In terms of business practices for SeaPort, decision authorities should request additional servers or larger servers to eliminate any bottleneck effect when high numbers of users are logged in and sending and receiving data in the SeaPort system. Furthermore, the servers should be designed to distribute the load in order to maximize the bandwidth and reduce the latency of the system

2. Currently, more and more data is kept and archived in the existing server taking up space in the readily accessible memory limiting the speed to which data can be accessed and passed along the server. Standard business practice should incorporate an archive plan, different than what already exists. Instead of retaining old files on the same server as the current and ongoing workload, a separate server specifically for storage and retention of archived data should be added to SeaPort.

3. In the event nothing would be able to fix SeaPort, it may be beneficial to use another software program or portal to issue large IDIQ service orders. Perhaps the Standard Procurement System (SPS) could accommodate and alleviate the issues SeaPort is experiencing?

## B. SUMMARY

To summarize this research we have found that there is evidence that cyber security plays a role in causing software applications like SeaPort to run inefficiently. Latency issues and document generations were the symptoms of this theory. Through literature research and survey analysis of professional workers using SeaPort, this data was used to support our theory that cyber security played a role in the problems of SeaPort. Unfortunately, due to the restrictions on cyber information on specific systems and networks within the DOD we can only conclude that there is a high possibility of a link between the increased focus on cyber security and poor performance of business systems used to support the warfighter. Therefore, with evidence of that link, it can be noted that cyber security measures may in fact be affecting the efficiency and effectiveness of the DOD's contract's writing staff and therefore inadvertently negatively impacting and endangering the programs and warfighter these cyber measures are in place to protect.

## C. AREAS FOR FURTHER RESEARCH

Based on our research, as well as experience, it is recommended that individuals in decision-making authority task cyber-security experts, who hold the proper access authority, to further investigate the link between cyber-security measures and SeaPort's performance issues. Another additional area of research we recommend would be to take a deeper look at the application of cloud-based servers in coordination with government systems. An in-depth look at the benefits of cloud-based servers, as well as potential pitfalls if use of these servers became more prevalent in the DOD, is also recommended.

# LIST OF REFERENCES


All sectors: Core Business Statistics Series: Advance Summary Statistics for the U.S. (2012 NAICS Basis): 2012. (2014, March 27). Retrieved April 21, 2016, from http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_00CADV1

Andrews, E. (2013, December 18). Who invented the Internet? Retrieved March 19, 2016, from http://www.history.com/news/ask-history/who-invented-the-Internet

Broad definition of "Cyber Threat" adopted by White House. (2013, February 15). Retrieved April 17, 2016, from http://reason.com/24-7/2013/02/15/broad-definition-of-cyber-threat-adopted

Brown, J. (2016, April 14). Report: Data breaches have exposed more than 851M records since 2005. Retrieved April 18, 2016, from http://www.ciodive.com/news/report-data-breaches-have-exposed-more-than-851m-records-since-2005-1/417399/

Bukszpan, D. (2015, September 25). The new era of cyberterrorism. Retrieved March 29, 2016, from http://www.cnbc.com/2015/09/25/

Carter, A. (2015, April 17). The DOD Cyber Strategy. Retrieved April 9, 2016, from http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DOD_CYBER_STRATEGY_for_web.pdf

Cobb, M. (2009, May 21). Balancing security and performance: protecting layer 7 on the network. Retrieved April 11, 2016, from http://searchsecurity.techtarget.com/video/Balancing-security-and-performance-Protecting-layer-7-on-the-network

Cross Domain Solutions. (n.d.). Retrieved April 21, 2016, from http://www.crossdomainsolutions.com/cyber-crime/

Day, G. (2015, April 3). How to increase operational efficiency in security? Executive Perspectives. Retrieved April 11, 2016, from https://www.fireeye.com/blog/executive-perspective/2015/04/how_to_increase_oper.html

Definition of cyberthreat in English:. (2016). Retrieved April 11, 2016, from http://www.oxforddictionaries.com/us/definition/american_english/cyberthreat

Deputy CNO. (2015, October 22). What the Navy is doing now to remain cybersecure. Retrieved April 07, 2016, from http://www.navy.mil/submit/display.asp?story_id=91679

Edwards, J., & Keiser, E. (2015, August 5). How DOD is making cyberattacks more costly, less successful. Retrieved April 9, 2016, from http://www.c4isrnet.com/story/military-tech/cyber/2015/08/05/raising-cost-cyberattacks/31173505/

Homeland Security. (2016, March 4). Retrieved April 11, 2016, from https://www.dhs.gov/how-do-i/protect-myself-cyber-attacks

How it works. (2016). Retrieved March 19, 2016, from http://www.internetsociety.org/Internet/how-it-works

Isaacson, C. (2014, September 24). Application scalability fundamentals - understanding big data scalability. Retrieved March 29, 2016, from http://www.tomsitpro.com/articles/understanding-big-data-scalability-book-excerpt,2-805-2.html

Khanse, A. (2014, December 02). Cyber attacks - definition, types, prevention. Retrieved March 10, 2016, from http://www.thewindowsclub.com/cyber-attacks-definition-types-prevention

Mukaram, A. (2014, June 02). Cyber threat landscape: basic overview and attack methods. Retrieved April 11, 2016, from https://www.recordedfuture.com/cyber-threat-landscape-basics

NAVSEA. (2001). Harnessing power, navigating change ... Retrieved March 29, 2016, from http://www.seaport.navy.mil/AboutUs/History.aspx

NCI. (2015, December 8). How to protect yourself from cyber-attacks [Infographic]. Retrieved April 23, 2016, from http://www.nationalcybersecurityinstitute.org/editorials/how-to-protect-yourself-from-cyber-attacks-infographic/

Office of Press Secretary. (2016, February 9). FACT SHEET: Cybersecurity National Action Plan. Retrieved April 9, 2016, from https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

OPM. (2015). Cybersecurity Resource Center Cybersecurity Incidents. Retrieved March 22, 2016, from https://www.opm.gov/cybersecurity/cybersecurity-incidents/

Reuters. (2016, April 15). U.S. Government ‘worse than all major industries’ on cybersecurity. Retrieved April 17, 2016, from http://www.nbcnews.com/tech/tech-news/u-s-government-worse-all-major-industries-cyber-security-n556461

Rouse, M. (n.d.). What is cybercrime? - Definition from WhatIs.com. Retrieved April 21, 2016, from http://searchsecurity.techtarget.com/definition/cybercrime

Sakole, J. (2015, November 11). Navy’s SeaPort-e solicitation means raised stakes for vendors. Retrieved April 21, 2016, from http://www.deltek.com/blog/home/b2g-essentials/2015/11/navys-seaport-e-solicitation-means-raised-stakes-for-vendors

Selinger, M., & Morgenstern, M. (2015, April 23). Endurance test: does antivirus software slow down PCs? Retrieved March 29, 2016, from https://www.av-test.org/en/news/news-single-view/endurance-test-does-antivirus-software-slow-down-pcs/

Software patches and OS updates. (n.d.). Retrieved April 17, 2016, from https://ist.mit.edu/security/patches

Sullivan, M. (2015, September 14). 8 types of business cyber attacks in business | QuickBooks. Retrieved March 22, 2016, from http://quickbooks.intuit.com/r/technology-and-security/8-types-of-cyber-attacks-your-business-needs-to-avoid/

UMUC. (2016). Cyber security primer. Retrieved March 19, 2016, from http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm

What is the Internet? (2016). Retrieved March 19, 2016, from http://www.internetbasics.gov.au/getting_started_on_the_Internet/what_is_the_Internet

What is SSL and TLS? (n.d.). Retrieved April 21, 2016, from https://www.symantec.com/page.jsp?id=ssl-information-center

THIS PAGE INTENTIONALLY LEFT BLANK

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California